We Claim:

1. A method for monitoring and controlling communications on a computer network, the computer network having a distribution node, comprising the steps of:

establishing a connection between a monitoring station and the computer network;

automatically retrieving a likely target file from the distribution node; and

automatically determining whether the likely target file contains illegal or undesirable content.

2. The method of claim 1, further comprising the step of automatically saving identification information for the distribution node.

3. The method of claim 2, wherein in the event that the automatically determining step establishes that the likely target file does contain illegal or undesirable content, the method further comprises the steps of:

automatically choosing an enforcement order; and

automatically executing the enforcement order against the distribution node.

4. The method of claim 3, wherein the enforcement order is an order to limit the network access of the distribution node.

5. The method of claim 3, wherein the step of automatically choosing an enforcement order comprises the steps of:

creating an electronic notice, the electronic notice comprising an identifier of the distribution node; and

using an enforcement rule to derive an enforcement order from the electronic notice.

6. The method of claim 1, wherein the automatically determining step further comprises the steps of:

automatically deriving a fingerprint from the likely target file;

automatically comparing the fingerprint with one or more previously stored fingerprints corresponding to one or more target files.

7. The method of claim 1, wherein the automatically determining step further comprises the step of:

automatically extracting a watermark from the likely target file.

8. The method of claim 1, wherein the automatically retrieving step, further includes the step of automatically identifying the likely target file.

9. The method of claim 8, wherein the step of automatically identifying a likely target file is performed based on one or more criteria chosen form the group of file name, file size, a hash value derived from the file, existing description of file contents, and metadata associated with the file.

10. A method for monitoring and controlling communications on a computer network, the computer network having a distribution node, comprising the steps of:

establishing a connection between a monitoring station and the computer network;

automatically retrieving a likely target file from the distribution node;

automatically determining whether the likely target file contains illegal or undesirable content;

automatically saving identification information for the distribution node;

automatically choosing an enforcement order; and

automatically executing the enforcement order against the distribution node.

11. A system for monitoring and control of communications over a computer network, comprising:

a plurality of network nodes;

a traffic controller, connected to the plurality of network nodes, and a computer network, and controlling a plurality of connections between the network nodes and the computer network;

a control station connected to the traffic controller; and

a monitoring station connected to the control station and the computer network,

wherein the monitoring station monitors whether illegal or undesirable content is being offered on the computer network, and in the event that such content is being offered sends electronic notices to the control station, the control station selects an enforcement order and the traffic controller executes the enforcement order by limiting access to the computer network from one or more of the plurality of network nodes.

12. The system of claim 11, wherein the monitoring station comprises a stored list of identifiers of illegal or undesirable content.

13. The system of claim 12, wherein the identifiers are fingerprints.

14. The system of claim 11, wherein the control station comprises a stored list of enforcement rules, and is configured to use the enforcement rules to derive enforcement orders from electronic notices.

15. The system of claim 11, wherein a plurality of traffic controllers and a plurality of monitoring stations are connected to the control station, and the control station chooses a destination traffic controller and sends the enforcement order to the destination traffic controller.

16. The system of claim 11, wherein a plurality of control stations are each connected to every one of the plurality of monitoring stations.

17. A device for monitoring and controlling network communications among several nodes on a computer network one of the nodes being a distribution node, comprising:

a processor; and

a memory storing processing instructions for controlling the processor, the processor operative with the processing instructions to:

establish a connection between the device and the computer network;

automatically retrieve a likely target file from the distribution node;

automatically determine whether the likely target file contains illegal or undesirable content;

automatically save identification information for the distribution node;

automatically choose an enforcement order; and

automatically execute the enforcement order against the distribution node.

18. The device of claim 17, wherein the memory further stores:

a plurality of enforcement rules; and

a plurality of enforcement orders.

19. A system for monitoring and controlling network communications among several nodes on a computer network one of the nodes being a distribution node, comprising a first device, the first device comprising:

a first processor; and

a first memory storing a first set of processing instructions for controlling first the processor, the first processor operative with the first set of processing instructions to:

establish a connection between the first device and the computer network;

automatically retrieve a likely target file from the distribution node;

automatically determine whether the likely target file contains illegal or undesirable content; and

automatically save identification information for the distribution node.

20. The system of claim 19, further comprising a second device the second device comprising:

a second processor; and

a second memory storing a second set of processing instructions for controlling the second processor, the second processor operative with the second set of processing instructions to automatically choose an enforcement order.

21. The system of claim 20, further comprising a second device the second device comprising:

a third processor; and

a third memory storing a third set of processing instructions for controlling the third processor, the third processor operative with the third set of processing instructions to automatically execute the enforcement order against the distribution node.